

OUCH!

Votre bulletin mensuel sur la sensibilisation à la sécurité

Les messages à faire et à ne pas faire

Aperçu

Envoyer des messages est un mode de communication essentiel dans notre vie personnelle et professionnelle. Cependant, nous sommes souvent notre pire ennemi lorsqu'il s'agit d'envoyer des SMS en toute sécurité. Découvrez les erreurs les plus courantes et comment les éviter dans votre vie quotidienne.

Le remplissage automatique

L'auto-complétion est une fonctionnalité courante dans de nombreuses applications de messagerie. Lorsque vous tapez le nom de la personne à qui vous voulez envoyer un message, votre application peut sélectionner automatiquement la personne pour vous. Cette fonction peut entraîner des erreurs, en particulier lorsque plusieurs contacts ont des noms similaires. Par exemple, vous pouvez avoir l'intention d'envoyer un SMS sensible à un collègue, mais l'envoyer accidentellement à l'entraîneur de votre fille, qui porte un nom très similaire. Vérifiez toujours le nom complet de la personne à qui vous souhaitez envoyer un message avant d'appuyer sur "Envoyer".

Répondre aux messages de groupe

Les discussions de groupe sont une autre fonctionnalité courante, mais assurez-vous de connaître tous les membres du groupe qui participent au fil de discussion avant de répondre. Lorsque vous répondez à un groupe entier, vous devez vous assurer que votre réponse est appropriée pour tous les membres de ce groupe. Une autre erreur fréquente consiste à répondre accidentellement à l'ensemble du groupe plutôt qu'à une personne en particulier. Prenez votre temps pour répondre : Vérifiez deux fois avant d'appuyer sur le bouton d'envoi.

Émotion

Évitez d'envoyer des messages lorsque vous êtes en colère, contrarié ou sous le coup de l'émotion. Ce message pourrait vous causer bien plus de tort à l'avenir, voire vous coûter une amitié ou un emploi. Au lieu de cela, prenez un moment pour organiser calmement vos pensées. Si vous devez exprimer votre frustration, ouvrez un nouveau message sans sélectionner de destinataire, écrivez exactement ce que vous ressentez, puis éloignez-vous de votre appareil. Vous pouvez aussi vous préparer une tasse de thé ou aller vous promener. Lorsque vous revenez, supprimez le message et recommencez. Vous serez probablement dans un état d'esprit beaucoup plus calme et clair. Envisagez une communication directe par téléphone ou en personne pour une conversation plus efficace. Il peut être difficile pour les gens de déterminer votre ton et vos intentions à partir d'un simple message texte.

La confidentialité

Les SMS traditionnels n'offrent pas de protection solide de la vie privée ; une fois le message envoyé, vous en perdez le contrôle. Les messages peuvent être transférés, affichés publiquement, partagés sous forme de capture d'écran, ou divulgués en vertu d'une décision de justice. Pour une communication privée, prenez le téléphone et appelez la personne. Enfin, si vous utilisez votre appareil professionnel pour la messagerie, n'oubliez pas que votre employeur peut être autorisé à surveiller et éventuellement à lire les messages sur les appareils professionnels.

Messages malveillants

Comme pour les e-mails, les cyber-attaquants vont essayer de vous piéger, de vous tromper ou de vous escroquer avec des messages. Ces messages peuvent contenir des liens malveillants sur lesquels ils veulent que vous cliquiez, des demandes de partage d'informations personnelles ou des pressions pour que vous appeliez un numéro de téléphone. Avez-vous déjà reçu un message texte étrange contenant uniquement le mot "Bonjour" et vous êtes-vous demandé de quoi il s'agissait ? Il s'agit d'un cyber-attaquant qui tente d'entamer une conversation avec vous, ce qui constitue souvent le début d'une escroquerie à la romance. Si vous recevez des messages étranges ou suspects sur votre appareil, supprimez-les simplement.

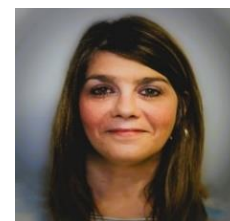
En outre, comme c'est le cas pour le courrier électronique, il est possible d'usurper la source d'un message texte. Assurez-vous de connaître l'identité de la personne avec laquelle vous envoyez un SMS avant de divulguer des informations personnelles, en particulier si vous n'êtes pas à l'origine de la conversation. Vous pouvez également bloquer tout numéro de téléphone ou compte indésirable ou suspect qui tente de vous envoyer un message.

Messagerie sécurisée

Assurez-vous que l'application de messagerie que vous utilisez est à jour et qu'elle dispose des dernières fonctions de sécurité. Envisagez d'utiliser des applications de messagerie sécurisée comme Signal pour renforcer la sécurité et la confidentialité.

Rédacteur Invité

Michele Tomasic, directrice adjointe de Women in Cybersecurity (WiCyS), est une dirigeante dynamique qui s'engage à faire progresser les femmes dans le domaine de la cybersécurité. Forte d'une solide expérience en matière de gestion des personnes et des opérations, elle met à profit son expertise pour promouvoir l'inclusion et la diversité et donner aux femmes les moyens d'agir au sein de la main-d'œuvre spécialisée dans la cybersécurité.



Ressources

Sécuriser vos appareils mobiles : <https://www.sans.org/security-awareness-training/ouch-newsletter/2018/securing-your-mobile-devices/>

Se débarrasser de vos appareils mobiles : <https://www.sans.org/newsletters/ouch/disposing-mobile-devices/>

Éviter les erreurs les plus courantes dans les e-mails : <https://www.sans.org/newsletters/ouch/avoid-the-most-common-email-mistakes/>

Signal : <https://signal.org>

Traduit pour la communauté par : Juliette Busson

OUCH! Est publié par SANS Security Awareness et est distribué sous la licence [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Vous êtes libre de partager ou de distribuer ce bulletin d'information, à condition de ne pas le vendre ou le modifier. Comité de rédaction : Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.